IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs. **CR. No. 16-4571 JCH**

GUY ROSENSCHEIN,

Defendant.

MEMORANDUM OPINION AND ORDER

This Memorandum Opinion and Order will address Defendant's *Motion to Suppress Evidence & Request for an Evidentiary Hearing under Franks v. Delaware* [Doc. 71], his *Updated Motion to Suppress Illegally Obtained Evidence for Lack of Probable Cause* [Doc. 254], and his *Motion to Suppress Evidence Due to Detective Hartsock's Unconstitutional Conduct* [Doc. 77]. On July 27-31, the Court held a week-long evidentiary hearing on the assortment of motions to suppress filed by Defendant, including those discussed here. Due to the COVID-19 pandemic, the hearing was held via videoconference and Defendant attended in the presence of his counsel. After reviewing the evidence presented at the hearing, all the of the briefs and exhibits filed by counsel, as well as the relevant legal precedent, the Court concludes that all three motions should be denied.

DISCUSSION

I. *Franks* Motions

In his *Motion to Suppress Evidence & Request for an Evidentiary Hearing under Franks v. Delaware* [Doc. 71] and *Updated Motion to Suppress Illegally Obtained Evidence for Lack of

Probable Cause [Doc. 254], Rosenschein asks the Court to suppress all evidence collected from the search of his home, as well as the fruits of all evidence collected from that search. As grounds for his motion, he contends that the search warrant was based on Bernalillo County Sheriff's Office Detective Kyle Hartsock's affidavit, which he alleges contained recklessly misleading information and omitted critical information that undermined the validity of the warrant. The Government filed a combined response [Doc. 82] to the original *Franks* motion as well as to two other motions to suppress. Rosenschein filed his consolidated reply brief. [Doc. 86]. On June 27, 2018, the Government filed a surreply [Doc. 94]. After additional discovery, Rosenschein revisited the *Franks* issue and filed his *Updated Motion to Suppress Illegally Obtained Evidence for Lack of Probable Cause* [Doc. 254]. This was followed by the Government's response [Doc. 278], *Dr. Rosenschein's Supplemental Brief in Support of His Suppression Motion Under Franks v. Delaware* [Doc. 293], the Government's response [Doc. 295], Rosenschein's reply [Doc. 299], and the Government's reply [Doc. 307].

A. Legal Standard

Defendants have a limited right to challenge in their criminal proceedings the truthfulness of statements made in an affidavit supporting an *ex parte* application for a search warrant. *See Franks v. Delaware*, 438 U.S. 154. 155-56 (1978). The court must hold a hearing on a *Franks* motion if the defendant first makes a showing that the affiant knowingly and intentionally, or with reckless disregard for the truth, included a false statement in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause. *Id*. Defendant must show that the affiant made intentional or reckless omissions as opposed to omissions negligently made or by innocent mistake. *United States v. Artez*, 389 F.3d 1106, 1116 (10th Cir. 2004).

"In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Franks*, 438 U.S. at 155-56. *Franks v. Delaware*'s standards apply to material omissions as well as to affirmative falsehoods. *See United States v. McKissick*, 204 F.3d 1282, 1297 (10th Cir. 2000)).

"If, however, the district court concludes that the omitted information would not have altered the magistrate judge's decision to authorize the search, then the fruits of the challenged search need not be suppressed." *United States v. Avery,* 295 F.3d 1158, 1167 (10th Cir. 2002), abrogated on other grounds, *United States v. O'Brien*, 560 U.S. 218, 235 (2010). "In a case where the defendant alleges information was intentionally omitted from an affidavit, the existence of probable cause is determined by examining the affidavit as if the omitted information had been included and determining whether the affidavit would still give rise to probable cause." *United States v. Basham*, 268 F.3d 1199, 1204 (10th Cir. 2001).

In this case, the Court did grant a hearing on the *Franks* motion. *See* Transcript of suppression hearing ("Tr.") 7/28/2020 at 5. At such a hearing, the burden is on the defendant to show by a preponderance of the evidence that "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause." *Franks*, 438 U.S. at 155-56.

B. Facts in Evidence

1. The Search Warrant Affidavit

On November 8, 2016, Detective Kyle Hartsock and others from the Bernalillo County Sheriff's Department searched Rosenschein's home for evidence of possession or distribution of child exploitation materials, including child pornography. They did so under a warrant to search the premises for evidence of child exploitation issued by state district court. That warrant was supported by the November 7, 2016, affidavit signed by Hartsock. [Ex. 12; Doc. 254-1; Hartsock, Tr., 7/28/2020 at 153].

According to Hartsock's affidavit, he has received classroom and on-the-job training in child abuse, sex crimes, and computer forensics. [Ex. 12 at 5]. The affidavit describes how Hartsock receives referrals from the New Mexico Attorney General's Internet Crimes Against Children and Human Trafficking ("ICAC") task force, which sometime gets subpoenas for address information from electronic service providers. It also describes how ICAC receives referrals from NCMEC. [Ex. 12 at 5.]. Regarding the nature of an IP address, Hartsock states that "[t]here are billions of possible IP addresses worldwide and no two internet capable electronic devices can share the same IP address at the same time. . . When a home residence [] wants internet access they open an account with an ISP [internet service provider] who then assigns an IP address to that account." [Ex. 12 at 5].

Hartsock's affidavit describes hash values thusly:

> Using hash values is another common technique used to identify users and specific electronic files. Hash values are mathematical algorithms that produce a 25-character pattern that is specific to a single file. These values have been proven to be unique and no two alike exist for different files. They are also not reverse engineerable, making them valuable to technology companies for encryption purposes. Law Enforcement has a database that tracks the hash values of known child pornography. By only having to look at a hash value and not the actual file, this makes the discovery of child pornography much more efficient.

[Ex. 12 at 5-6]. The affidavit does not state that it was Microsoft's cloud-based PhotoDNA software system that made the hash value match in this case. [Hartsock, Tr. 7/28/2020 at 158-59].

In his affidavit, Hartsock describes Chatstep as follows:

> Chatstep.com is a website located on the public internet. The company is located in the United States. It allows visitors to the website to look at "Public" chat rooms and join them. The public chat rooms are required to have names that their creator gives them. Up to 50 users can be in a chat room at the same time. A user can enter a public, already created chat room, or create their own. The rooms can be private or public to other users. Once in a room of more than 2 users, a user can send a personal message to just one user to have a private, one on one conversation.

[Ex. 12 at 6.] Regarding the incident of July 31, 2016, Hartsock wrote:

> On July 31, 2016 Chatstep.com reported that a user with the temporary name of "Carlo" had uploaded an image of child pornography and sent it to another user. The IP address used in the upload was 75.173.104.251. Chatstep provided the photograph that was uploaded. I reviewed it and it does depict a child under 18 years old involved in a sex act. A grand jury subpoena was given to the internet service provider asking for the subscriber of this IP at the exact date and time of the upload to be identified.

[Ex. 12 at 6]. Hartsock then set forth the user information provided to him by the internet service provider, CenturyLink, in response to the grand jury subpoena. That information included the user ID "rosenscheinguy" as well as Rosenschein's full name and Albuquerque address. [Ex. 12 at 7].

The affidavit contains substantially identical information regarding the August 8, 2016 incident, except for a different date and IP address, 75.173.102.112. [Ex. 12 at 7-8]. Hartsock stated that he had also viewed the second image. [Ex. 12 at 7].

2. Evidence Presented at the Hearing

The Court incorporates herein all of its factual findings in its Memorandum Opinion and Order dated November 12, 2020. [Doc. 319].

In 2016, Hartsock was a certified digital evidence examiner with a unit of the Bernalillo County Sheriff's Department focused on child exploitation and human trafficking. [Hartsock, Tr. 7/28/2020 at 118]. Around November 2, 2016, the New Mexico Attorney General's Office's Internet Crimes Against Children ("ICAC") task force reached out to Rosenschein to assign him Cybertips that had been referred for investigation by the National Center for Missing and Exploited Children ("NCMEC"). [Id. at 125-26, 130]. After the CyberTips were assigned to him, Hartsock learned that ICAC had already received a grand jury subpoena for internet service provider CenturyLink to pinpoint two IP addresses relating to the CyberTips. [Id. at 130-31]. In response to the subpoena, CenturyLink associated the two IP addresses to a name and an address—Rosenschein's residence in Albuquerque, New Mexico. [Id. at 131, 161, 256]. In his experience, Hartsock had found this process to be reliable. [Id. at 131-32]. Hartsock was not involved in obtaining the state grand jury subpoenas, however. [Id. at 131].

The task of securing a grand jury subpoena to obtain CenturyLink's records relating to the IP addresses in the CyberTips fell to Marla Richards, a criminal analyst for ICAC. [Richards, Tr. 7/29/2020 at 225]. Though she does not recall these two images specifically, it was her practice to open images attached to CyberTips after she received them from NCMEC. [Id. at 230]. At that time in late 2016, it was not standard practice in the ICAC to get a warrant before opening images attached to CyberTips. [Id. at 243-44]. Richards testified that she probably wrote an affidavit to support the requests for grand jury subpoenas for the IP addresses and other data associated with the CyberTips in question, as it was her standard practice to do so. [Id. at 236-237, 241]. In her grand jury testimony, Richards gave the members of the grand jury a description of the images. [Id. at 241]. Richards testified credibly that she did not know she needed a warrant to open the images, but even if she had known that she had opened the images illegally—or even if she did not have the images at all—she still would have pursued the grand jury subpoena in this case for information from CenturyLink based solely on the fact of the hash matches and the known IP addresses. [Id. at 244-46; 252-53]. Based on her experience in obtaining grand jury subpoenas, she believed that even under those circumstances subpoenas would have been granted. [Id. at 245-46]. Richards further testified that she was certain she would have sought a subpoena based solely on a CyberTip without an image or mention of hash match, and it likely would have issued. [Id. at 252-53].

In any event, when ICAC passed the case along to Hartsock, it included the subscriber information obtained from CenturyLink via the grand jury subpoenas. When he wrote the affidavit at issue, Hartsock was familiar with CyberTips coming from electronic service providers based on hash matches. [Hartsock, Tr. 7/28/2020 at 127-28]. He understood the basic concept of hash matching and testified that in his experience, hash matches were "100 percent reliable." [Id. at 128-30]. After reading the CyberTip Reports forwarded by NCMEC and ICAC, Hartsock felt confident that the images were very likely child pornography because of the reliability of hash matching and the fact that the CyberTip report described the "incident type" as "child pornography, unconfirmed." [Id. at 233-35]. In his experience, the images attached to reports derived from hash matching and with that incident type always turned out to be child pornography. [Id. at 235; Hartsock, Tr. 7/29/2020 at 20-21].

Reading the two CyberTip reports in this case, Hartsock realized that they were based on hash matches recognized by PhotoDNA, that the incident type was "child pornography," that the match was based on a file that was uploaded to Chatstep's server, and that NCMEC had not reviewed the files; further, Hartsock understood PhotoDNA to be a hashing service and that it was reliable. [Id. at 133-35, 140-41; Exs. 10 and 11]. Hartsock believed Chatstep's tip to be credible because it was based on a hash match. [Hartsock, Tr. 7/29/2020 at 20]. The two CyberTip reports [Exs. 10 and 11] were both submitted by Chatstep and identified a user named "Carlo." [Hartsock, Tr. 7/28/2020 at 136-37, 141-42] Further, the CyberTips contained two different IP addresses, but they were associated with the same physical address in Albuquerque. [Id. at 138-39, 142]. Hartsock was not concerned that two different IP addresses had pointed to the same physical address because it is common for electronic service providers to use dynamic IP addresses, which can change at any time. [Id. at 142]. Neither CyberTip included the content of communications between Carlo and another person, nor did either tip contain any image that did not result in a hash match. [Id. at 139-40, 143].

Consistent with his standard procedure, Hartsock reviewed both the CyberTip reports and the associated images, and he did so without a warrant. [Hartsock, Tr. 7/28/2020 at 143-44, 146]. He looked at the images because "knowing [] the type of sexual assault that's being memorialized in a photo can assist in [his] interview of subjects on scene." [Id. at 145]. Hartsock did not obtain a warrant before looking at the images because he had never done that before with a CyberTip, the files had already been opened by the Attorney General's ICAC task force, and subpoenas had been served on the internet service provider. [Id. at 146]. At that time, it was not Hartsock's practice to get a warrant before reviewing images. [Id.]. Rather, it was his normal practice in cases of CyberTips coming from NCMEC to open and view the files attached to the CyberTip Reports. [Id. at 232-33]. In this case, that is what he did, and both images appeared to portray the sexual assault of pre-pubescent male by an adult male, possibly from the same incident. [Id. at 145-46].

In his affidavit, Hartsock did not mention PhotoDNA or Microsoft. He testified that he did not identify that it was Microsoft's PhotoDNA software that triggered the hash match because he did not believe that the specific type of hashing software used was necessary to the question of probable cause since in his view all types of hashing had been shown to be reliable. [Hartsock, Tr. 7/28/2020 at 158-59]. For that same reason, he wrote that there had been a report of child pornography rather than a report of a hash match to known child pornography—in his estimation, they were the same. [Id. at 173-74]. In the portion of the affidavit containing facts specific to this case, Hartsock did not mention NCMEC, although he did mention it earlier in the affidavit with regard to its role in gathering and distributing online tips to the relevant state ICACs, which then conduct an investigation. [Ex. 12 at 5; Hartsock, Tr. 7/28/2020 at 174-75]. Hartsock did not use the word "CyberTip," but he did describe the contents of the CyberTips. [Hartsock, Tr. at 243-44].

On August 9, 2016—approximately two months before beginning his investigation in this case—Hartsock received an email from an assistant attorney general informing him and others of the Tenth Circuit's decision in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) and attaching a copy of the "extremely adverse opinion." [Ex. 9]. Hartsock quickly reviewed the email and the *Ackerman* opinion, and seven minutes later he responded to the assistant AG as follows:

> "Seems that if [*Ackerman*] isn't appealed or overturned, they would simply stop opening the attachments and rely on the hash match, then we would have to write a warrant, etc. to get files. Or the other companies would need to open the files themselves, therefore NCMEC is merely repeating the private search. But to clarify, nothing we can really do about this right now, it's a NCMEC issue?"

[Ex. 9; Hartsock, Tr. 7/28/2020 at 146-47]. Even though he had just a few minutes to skim the opinion and draft his email in response, Hartsock's message shows an accurate grasp of the import of *Ackerman*. Hartsock testified that in writing this email, he was seeking guidance from the various prosecutors who were copied. [Id. at 147, 216]. He had the impression that the opinion primarily affected NCMEC. [Id. at 195-96; Hartsock, Tr. 7/29/2020 at 16, 18]. Hartsock did not think it affected the way he investigated child exploitation cases on a day-to-day basis, and no one responded to his message directing him to change his procedures at any time before he performed his investigation in this case. [Id. at 149. 195-96]. If he had known with certainty that *Ackerman* applied to his opening of images attached to CyberTips stemming from a hash match, he simply would have written a search warrant before opening them, as he has done since receiving guidance on the ramifications of the *Ackerman* opinion. [Id. at 151-52]. Since adopting that procedure, no judge has rejected one of his applications for search warrant based solely on a hash match. [Id. at 152]. Hartsock testified that if he had known in November of 2016 that he needed a warrant to look at the images in this case, he simply would have obtained one based on the hash match (as is his current practice) and continued with his investigation in the normal course by viewing the images. [Id. at 152-53]. However, he felt that the Attorney General's office was generally opening and reviewing images of suspected child pornography before referring cases to him, so Hartsock did not believe that *Ackerman* would really affect the way he conducted investigations. [Id. at 215].

C. Analysis

Rosenschein argues that "[o]nce the recklessly misleading information in the affidavit is excluded, there is insufficient evidence to establish a finding of probable cause. The resulting language fails to conclusively show that the images involved were in fact child pornography and fails to connect the unnamed digital image files to Dr. Rosenschein or his residence . . ." [Doc. 245 at 3]. He asks for the search warrant to be voided and the evidence found at his residence suppressed. Rosenschein further requests that the grand jury subpoena be suppressed. [Id.].

1. Intentionally and recklessly false statements[1]

Rosenschein makes a series of arguments asserting that Hartsock's affidavit contained intentionally and recklessly false statements. First, he argues that Hartsock falsely stated that "[u]sing hash values is another common technique used to identify users and specific electronic files." Rosenschein argues that hash values can be used to identify particular files, but they cannot identify individual users. [*See* Doc. 254 at 8]. However, as the Government points out, electronic service providers use hashing technology on usernames, passwords, and email addresses—pieces of information that generally link to specific users—as a way to keep those pieces of data secure when being sent over the internet. [Hartsock, Tr. 7/28/2020 at 157-58]. An ESP can use a hash value to determine what user was logged in and saved or uploaded a particular file. [Doc. 278 at 9-10; Hartsock, Tr. 7/28/2020 at 156-58]. Thus, Hartsock's statement is accurate. The next sentence of the affidavit states, "[h]ash values are mathematical algorithms that produce a 25-character pattern that is specific to a single file." Rosenschein points out, and the Government does not dispute, that hash values are not actual algorithms[2], and not all hash values are 25 characters in length. With the false words excised, the statement reads, "hash values are . . . a . . . character pattern that is specific to a single file." Although Rosenschein admits that omission of the incorrect

[1] In his brief, Rosenschein categorizes the alleged problems with Hartsock's affidavit as "false statements," "misleading statements," and "material omissions." [Doc. 254]. It appears that Rosenschein may have placed some of his arguments under the incorrect headings. For example, his discussion under "false statements" contains some arguments about material omissions. Nevertheless, the Court addresses each category of arguments in turn, following them in the same order and under the same headings presented by the Defendant.

[2] The Government argues that while hash values are not algorithms, the word algorithm is often used *in reference* to a hash value. This argument is unconvincing. It is inaccurate to call a hash value an algorithm, when in fact hash values are the product of algorithms. But as explained herein, this technical inaccuracy does not affect the probable cause determination.

information may not negate probable cause, he argues that its inclusion demonstrates either Hartsock's intent to mislead the court, or his reckless disregard for the truth. [Doc. 254 at 9].

The Court disagrees with Rosenschein's assertion that these technical inaccuracies in Hartsock's affidavit demonstrate an intent to mislead the court or a reckless disregard for the truth. While Hartsock may have had some training in computer forensics, he is hardly an expert in that field. It is not entirely surprising that he misapprehended some of the details and language of hash match technology. The Court found Hartsock's testimony to be credible, and it detected in him no intent to mislead. Perhaps most importantly, aside from Hartsock's subjective intent, these misstatements did not mislead the court in any meaningful way. Whether or not a hash value is an algorithm or the product of an algorithm, or the number of characters in a particular hash, is not the point. Rather, the salient point for purpose of a probable cause determination is that a hash value is unique to any given image and thus is a reliable way to identify an image—and the affidavit makes that point clear. Further, the inaccuracies do not appear to have made the issuing court any more likely to find the existence of probable cause to search. The fact is that hash values are "specific to a single file" and "proven to be unique," which is how Hartsock describes them in his affidavit. With the inaccurate information excised as noted above, the affidavit still would support probable cause.

Rosenschein asserts that the "most egregiously false statements" in Hartsock's affidavit are those in which he stated that "Chatstep.com reported that a user with the temporary name of 'Carlo' had uploaded an image of child pornography and sent it to another user." [Doc. 254 at 9]. Rosenschein asserts that this was egregiously false because it was NCMEC that provided the reports, not Chatstep. [Id.] However, the evidence at the hearing demonstrated that Hartsock's statement was accurate: Chatstep made the report, which Microsoft routed to NCMEC, and which

NCMEC then forwarded to the New Mexico Attorney General's Office. [Doc. 319 at 8, 15; Richards, Tr. 7/29/2020 at 227-28].

Next, Rosenschein takes issue with Hartsock's description of CyberTips as "online tips of sexual predators that have possibly committed a crime" [Doc. 254 at 9], because NCMEC had not viewed the images attached to the CyberTips or conducted an investigation of the tips, and because Hartsock failed to follow up with NCMEC to verify any of the information in the CyberTips or conduct an independent investigation before seeking the search warrant. However, the Court is unaware of any requirement that a law enforcement officer like Hartsock conduct further investigation after receiving a CyberTip and information from a grand jury subpoena. After all, the requirement for a search warrant is probable cause, and such warrants are often obtained during the court of an investigation, not necessarily at its conclusion. The affiant in a warrant application need not exhaust every possible lead, nor must the affidavit contain all the information that law enforcement could ever possibly obtain in relation to a suspected crime. All that is required is probable cause.

Rosenschein asserts that Hartsock incorrectly stated that Carlo had "uploaded" an image. According to Rosenschein, because PhotoDNA hash-matched the image to a known image of child pornography, the image was blocked, never transmitted to another person on Chatstep, and therefore was never "uploaded." Again, the Court disagrees based on the evidence. For the image to have been hashed by PhotoDNA, "Carlo" had to transmit the image from his own device to the Chatstep server. [*See* Ex. 1 at ¶ 10 ("The Match API permits the developer [Chatstep] to transmit images to Microsoft's proprietary cloud environment, where those images are hashed.")]. This constitutes an upload of the image. In addition, the CyberTipline reports (which Hartsock would have no reason to question) describe the images as "uploaded files." [Exs. 10 and 11 at 1].

Next, Rosenschein argues that Hartsock misled the court by not describing Microsoft PhotoDNA or mentioning that the submitters of the CyberTips were Chatstep.com, Microsoft-PhotoDNA Cloud Service on behalf of Carlo@Chatstep.com, and "105Labs, LLC," as indicated in the CyberTipline Reports. Rosenschein does not explain how this information would have altered the judge's probable cause analysis, and the Court posits that it is because the information is not particularly material to the issue. Rosenschein asserts that Hartsock's statement that "Chatstep.com reported that a user with the temporary name of 'Carlo' had uploaded an image of child pornography and sent it to another user" was "intentionally false." [Doc. 254 at 11]. The Court disagrees. First, that information is essentially what is contained in each of the CyberTips. Second, while it may be technically true that Carlo uploaded the images to Chatstep and that they were intercepted before transfer to "another user," that fact does nothing to alter the conclusion that there was probable cause to believe that "Carlo" possessed and either distributed or attempted to distribute child pornography; another Chatstep users receipt of the images does not affect the probable cause determination. And third, there is no evidence that Hartsock intentionally misled the court on this point. In fact, Hartsock credibly testified that at the time he wrote the affidavit, he did not know that Chatstep quarantined any image that was hash-matched to known child pornography before it could be sent to others. [Hartsock, Tr. 7/28/2020 at 173; Tr. 7/29/2020 at 12-13]. This was his first encounter with Chatstep, so Hartsock also did not know how PhotoDNA operated within Chatstep, whether images were intercepted, or whether anyone at Chatstep opened images linked to a CyberTip. [Hartsock, Tr. 7/28/2020 at 164-65, 168]. There is simply no evidence of intent to mislead.

Rosenschein asserts that Hartsock was aware that PhotoDNA (created by Microsoft) had obtained the images "without a warrant in violation of the Fourth Amendment" but failed to mention this in his affidavit. This argument is also without merit. Hartsock had no knowledge as to whether or not either Chatstep or Microsoft had obtained a warrant, so he would have no reason to mention it. [Hartsock, Tr. 7/28/2020 at 168-69]. Furthermore, Microsoft is a private company, so Hartsock would not have reason to believe that it needed a warrant to obtain images or forward them to NCMEC.

Rosenschein contends that Hartsock intentionally misled the Court by saying that he had "reviewed" the images attached to the CyberTips. According to Rosenschein, Hartsock used that word to imply—falsely—that Chatstep had previously viewed the images, such that by looking at them himself Hartsock was *re*viewing them. First, this argument is contrary to common English usage in context of the affidavit, in which the term "review" would normally be used to mean "to look at." No one would reasonably interpret Hartsock's choice of word in this context to mean that he was viewing the images after someone else had viewed them. Second, Hartsock testified quite credibly that when he used that word, he was not suggesting that someone else had previously viewed the images, but rather that he himself looked at them. [Hartsock, Tr. 7/28/2020 at 175-76]. Rosenschein's argument is unconvincing as to both whether the judge was actually misled and whether Hartsock intended to mislead him.

Rosenschein's penultimate argument is that by failing to mention the CyberTips, NCMEC, or Microsoft in his warrant affidavit, Hartsock intentionally created the false impression that the images had been viewed by Chatstep and identified as child pornography, whereas the CyberTip Reports described them as "unconfirmed" images of child pornography. [Doc. 254 at 13]. It appears that Rosenschein is suggesting that Hartsock misled the judge into believing that there was certainty that the images contained child pornography, when in reality their contents were unconfirmed. This argument overlooks the fact that Hartsock viewed the images himself and told the judge that he had done so, describing them as depicting a child under 18 involved in a sex act. [Ex. 12 at 6-7]. Therefore, Hartsock did not mislead the judge as to whether there was any doubt about the contents of the images.

Finally, Rosenschein contends that the Government has failed to present chain of custody evidence demonstrating that the images in his possession were the same images uploaded to and reported by Chatstep and that Hartsock failed to corroborate the two IP addresses found in the CyberTipline Reports. [Doc. 254 at 13]. Again, the Court finds that this argument illuminates no intentionally or recklessly false statements by Hartsock. If anything, the evidence demonstrates the accuracy of Hartsock's affidavit, to wit: Chatstep identified the IP addresses used by "Carlo" to upload the two images and included those addresses in its CyberTips, and the internet service provider stated that both IP addresses pointed to Rosenschein's home. These facts remain true. Further, evidence obtained by law enforcement after the search further corroborates chain of custody. Rosenschein admitted to using Chatstep and the name "Carlo," [Hartsock, Tr. 7/28/2020 at 183-84], and police found in Rosenschein's possession an image that appeared to be from the same series of photos as those attached to the CyberTips, in that they portrayed the same male victim, the same setting, and the same, distinct bedspread. [Id. at 181-82]. In short, there does not appear to be a chain of custody problem, but even if there were, it would not require suppression under *Franks*.

2. Misleading statements

Rosenschein argues that Hartsock exaggerated the information in the affidavit to bolster probable cause and mislead the judge. First, he contends that Hartsock "hid" Microsoft and NCMEC's involvement from the Court. But Hartsock described NCMEC's CyberTipline process, stated that NCMEC forwards CyberTipline Reports to the state ICAC, and that hash values are used to identify images previously identified as contraband. [Ex. 12 at 5-6]. A few paragraphs later, Hartsock also described the process by which Chatstep "reported" that "Carlo" had uploaded an image of child pornography. [Id. at 6]. The way the affidavit is written, a reasonable reader would infer that this report took place via NCMEC's CyberTipline—which is true. While Hartsock did not explicitly discuss Microsoft's PhotoDNA Cloud Service in his affidavit, it's unclear to this Court how that omission misled the issuing court on the question of probable cause. Indeed, as the Government correctly points out, courts have upheld search warrants that mention a hash match but do not detail the technical, automated process that led to the match. *See, e.g., United States v. Arumugam*, 2020 WL 1154651 at *5 (W.D. Wash. Mar. 10, 2020) (concluding that "any omissions in the affidavit regarding technical details of [the digital hash-matching program] and its automated operations were not material to the probable cause inquiry."); *United States v. Thomas*, 2013 WL 6000484 at *24 (D. Vt. Nov. 8, 2013) (observing that affidavit established probable cause even without evidence that defendant made a direct download of contraband files because "courts have consistently found probable cause exists when an IP address that appears to have accessed child pornography can be traced to an identifiable residence.").

Next Rosenschein argues that Hartsock made a false statement when he averred, "no two internet capable electronic devices can share the same IP address at the same time." [Doc. 254 at 15; Ex. 12 at 5]. He contends that multiple users can connect to the same router and thereafter "appear under the router's IP address." However, as the Tenth Circuit explained in *United States v. Henderson*, "[a]n IP address is a unique number identifying the location of an end[-]user's computer. When an end-user logs onto an internet service provider, they are assigned a unique IP number that will be used for that entire session. Only one computer can use a particular IP address at any specific date and time." 595 F.3d 1198, 1199 n.1 (10th Cir. 2010) (alterations and quotations omitted). Wi-Fi routers—such as those in private residences—have a single public IP address to communicate with the internet but then assign individual, unique, private IP addresses to each device that connects to that router. [Hartsock, Tr. 7/28/2020 at 160-61. Thus, no two devices are ever using the same private IP address at the same time, and Hartsock's affidavit was not misleading on this point.

Rosenschein asserts that by stating, "[w]hen a home residence or business wants internet access they open an account with an ISP who then assigns an IP address to that account," Hartsock falsely implied that an IP address corresponds to a specific geographical location. [Doc. 254 at 15]. According to Rosenschein, a person could move their router to a different physical location, but the IP address would remain the same. [Id.]. First, the Court disagrees with the assertion that the quoted statement from Hartsock's affidavit implies that an IP address is associated with a fixed geographical location. The statement plainly says that the IP address is assigned to a user's "account." Second, it is not correct that one can simply move one's router to a different location, plug it in, and continue using it with the same IP address. Rather, one must contact the internet service provider, give them the router's unique MAC address, and request them to authorize service. [Hartsock, Tr. 7/28/2020 at 162-63; *see also United States v. Knowles*, 207 F. Supp. 3d 585, 590 (D.S.C. 2016) ("A MAC address is assigned to a network interface, usually by the manufacturer, to identify devices on a network.")]. At that point, the internet service provider has a record of the new address and would assign the router a public IP address.

Rosenschein takes issue with Hartsock's statement that Chatstep "allows visitors to the website to look at 'public' chatrooms and join them," and that the public chat rooms are "required to have names that their creator gives them." According to Rosenschein, this falsely implies that a user can see the content of a chatroom before joining it. While this Court does not read the statement that way, it will assume for the sake of argument that the judge who received the warrant affidavit did so. The fact remains that such an interpretation would do nothing to alter a finding of probable cause to conclude that someone at the physical address in Albuquerque corresponding to the two IP addresses on the CyberTip Reports uploaded a hash-matched image of child pornography using Chatstep. Whether or not a Chatstep user can see the content of a chatroom before entering it simply does not alter that determination. The same is true of Rosenschein's complaint that "Hartsock failed to inform the judge that a visitor may leave the chatroom without closing it, thereby appearing on the chatroom's user list while not actually present." [Doc. 254 at 16]. Whether or not "Carlo" was on any specific chatroom's user list or was actively participating in any particular chat room (rather than being passively logged in, but away from his computer) is simply not a fact relied on or relevant to a finding of probable cause to believe that someone at the searched Albuquerque residence *uploaded* an image of child pornography. Thus, Hartsock's "failure" to inform the judge of this fact was immaterial.

Rosenschein's final complaint is with Hartsock's statement that "once in a room of more than 2 users, a user can send a personal message to just one user to have a private, one on one conversation." [Doc. 254 at 16]. He contends that the statement erroneously suggests that there must be at least two people in a room in order for one of them to send messages, when in fact a user in a room by himself can post a message or image for only himself to see. While that hypothetical scenario is possible in theory, it is not otherwise helpful to a probable cause determination. As the Government suggests, such a scenario is incompatible with the fundamental notion of a chatroom, the purpose of which is to share information with others. But even more importantly, the statement is irrelevant to a probable cause determination. Here, all Hartsock had to do was demonstrate that there was evidence supporting probable cause to believe someone in the Albuquerque residence possessed child pornography and/or attempted to distribute it by uploading it to a Chatstep server. He did not need to demonstrate that another Chatstep user actually viewed the images.

3. Material Omissions

Rosenschein urges the Court to find that Hartsock's affidavit omitted material information that should have been provided to the judge authorizing the search warrant. His primary argument is that Hartsock "failed to inform the court that his affidavit was based upon information procured through Fourth Amendment violations." [Doc. 254 at 16-17]. Specifically, Rosenschein contends that Hartsock should have told the judge that the grand jury subpoena of CenturyLink records from which Hartsock obtained Rosenschein's name and address was illegal because it was procured as a result of an unconstitutional, warrantless viewing of the images attached to the two CyberTip Reports in this case. In addition, Rosenschein argues that Hartsock should have informed the judge that he too viewed the images without a warrant, and that the evidence was based on a prior unlawful search under *Ackerman*. [*See also* Doc. 293 at 3-4].

In its prior Memorandum Opinion and Order, this Court concluded that when Hartsock opened and viewed the images attached to the CyberTip Reports, he merely repeated the earlier private search performed by private actors Microsoft and Chatstep. [Doc. 319 at 24-28]. The Court also found that Rosenschein failed to demonstrate that he had a constitutionally protected privacy interest in the two images he uploaded onto a public chat site. [Doc. 319 at 8-11]. Because he was repeating a private search and because Rosenschein lacked a cognizable privacy interest in the images, Hartsock did not need a warrant to view them, and he did not violate the Fourth Amendment. Rosenschein offers no reason that the Court should reach a different conclusion as to the search performed by the ICAC officers who viewed the images before they obtained the grand jury subpoena.

Further, Rosenschein's reliance upon *Ackerman* in this instance is misplaced. In that case, internet service provider AOL found a hash match for an image attached to an email that one of its users attempted to send. As part of its CyberTip Report, AOL forwarded to NCMEC not only the hash-matched photo, but also the body of the email and three other attached photos that had not been hash-matched to known images of child pornography. 831 F.3d at 1294. The Tenth Circuit expressed concern over the constitutionality of a NCMEC analyst opening and reading emails, as well as the attached photos, without a warrant when neither the emails nor photos been previously viewed by any private person or entity. *Id*. at 1306. Those are not the facts here, where neither Rosenschein's written communications nor any photos that were not hash-matched have been viewed without a warrant. In this case, law enforcement viewed only the two photographs that were uploaded to Chatstep and hash matched by PhotoDNA, and thus they fell within the private search doctrine. In fact, the *Ackerman* court expressly declined to address the situation presented here. *Id*. at 1306-07. As a result of the foregoing, Hartsock's failure to inform the judge reviewing his affidavit that no one at Chatstep had reviewed the images and decided they were child pornography is not material because "*Ackerman*'s limits on police power" were not at play. Furthermore, Hartsock's failure to mention the fact that he had viewed the images without a warrant does not suggest nefarious intent because he was simply following his department's and his own established practices at the time. [Hartsock, Tr. 7/28/2020 at 233].

Next, Rosenschein argues that Hartsock failed to inform the judge that the two images were reported as *possible* child pornography without being viewed by a human. [Doc. 254 at 18]. It is true that the CyberTips in this case stated that the "incident type" was "Child Pornography

(Unconfirmed—Files Not Reviewed by NCMEC)". However, this would have been of little significance to the judge's probable cause determination because at least one human—Detective Hartsock—did review the images and determine that they involved a minor involved in a sex act. As already explained, Hartsock's viewing of the images did not violate the constitution, and by describing their contents to the judge Hartsock altered their status from being merely potentially illegal to very likely illegal. Thus, the fact that no one viewed the images until they got to New Mexico would not have altered the probable cause analysis.

Rosenschein argues that Hartsock failed to inform the judge that he did not call Chatstep to independently confirm that the IP addresses listed in the CyberTips were actually used on Chatstep's website, and that Hartsock failed to report that the IP addresses were never verified by an investigating agency. However, it was Chatstep that provided the IP addresses in its CyberTipline Report, and Hartsock accurately recounts those addresses in his affidavit. There is no evidence to suggest that Chatstep was unreliable in its reporting of IP addresses or that Hartsock had any reason to question its accuracy. The Court strains to see how the fact that Hartsock did not tell the judge that he did not call Chatstep to confirm the IP addresses would have influenced the probable cause determination. Further, in response to the grand jury subpoena, the internet service provider produced information linking those IP addresses to Rosenschein's address and user ID "rosenscheinguy." Hartsock accurately provided that information to the magistrate judge as well. Altogether, this recitation of facts demonstrates a nexus between Rosenschein's home and the IP addresses linked to the uploaded photos and does not omit material information.

Lastly, Rosenschein contends that Hartsock failed to describe the images with the required specificity. Hartsock stated that the images "depict a child under 18 years old involved in a sex act." [Ex. 12 at 6]. Rosenschein contends that this language is too conclusory for the judge to make an independent determination that the images are child pornography, and that he should have provided either a detailed description or attached the images themselves.

The cases Rosenschein cites do not support his position, however. In those cases, courts had rejected officers' conclusory descriptions of images that merely parroted the applicable statutes, finding them to be inadequate. *See, e.g., United States v. Brunette*, 256 F.3d 14, 18 (1st Cir. 2001) ("pre-pubescent boy lasciviously displaying his genitals" was inadequate description of images, where that description is identical to statute and a determination of whether display was "lascivious" required more information); *United States v. Doyle*, 650 F.3d 460, 474 (4th Cir. 2011) (description of images as "nude children" was insufficient to establish probable cause for suspected child pornography); *United States v. Pavulak*, 700 F.3d 651, 661-62 (3rd Cir. 2012) (conclusory description of images as "child pornography" without any supporting details was insufficient); *United States v. German*, 3:15-cr-00101-wmc, Doc. 34 at 8 (W.D. Wis. Feb. 2, 2016) (unpublished) (finding inadequate description where agent described images only as "child pornography" and did not state whether he had reviewed them himself).

These cases relied upon by Rosenschein are unlike the circumstances here, in which Hartsock stated that the images were of a child under 18 involved in a sex act. Far from being a conclusory statement of "child pornography," Hartsock's statement sets forth a description the age of the person depicted (a child under 18) and what they were doing (participating in a sex act). That is a far cry from simply labeling photographs as child pornography. In fact, in another case cited by Rosenschein the Tenth Circuit required no more than a general description, *United States v. Simpson*, 152 F.3d 1241, 1246-47 (10th Cir. 1998) (concluding that description of images as "child pornography" was sufficient to support probable cause). Further, Hartsock testified that he had used the same or similar descriptions in other search warrant affidavits without any problems, but that if the judge had wanted a more detailed description, he would have provided it. [Hartsock, Tr. 7/28/2020 at 171-72]. Thus, the Court concludes that Hartsock's description of the images was adequate.

4. Hartsock's Email

In a supplement to his motion [Doc. 293], Rosenschein argues that Hartsock's August 9, 2016 email to prosecutors regarding the Tenth Circuit's *Ackerman* decision showed that he was not only aware of the opinion but also understood it to prohibit him from opening the images attached to CyberTip Reports without a warrant. Rosenschein contends that "[k]nowing that he and his fellow local law enforcement officers should have obtained a warrant before looking at the images, Detective Hartsock drafted a severely misleading if not intentionally false affidavit to a state court judge in order to convince that judge to issue a warrant for Dr. Rosenschein's home." [Doc. 293 at 2-3].

However, as previously discussed by the Court, this argument fails for three reasons. First, law enforcement did not in fact require a warrant to view the images because Rosenschein lacked a cognizable privacy interest in those images, and because law enforcement was merely repeating a private search. Therefore, there was no legal reason for Hartsock to inform the judge that he and ICAC viewed the images without first obtaining a warrant. Second, as the Court has previously discussed herein, Hartsock's affidavit was not false or misleading in any material way. Third, after reviewing the exhibits and considering Hartsock's testimony, the Court concludes that he had no subjective intent to mislead the judge who issued the search warrant. Rather, the Court finds credible Hartsock's testimony that he believed the *Ackerman* opinion to have affected NCMEC but not to have altered the then-established practices and procedures he followed in the child pornography cases he investigated. And of course as the Court has already noted, the *Ackerman* opinion expressly declined to address the circumstances presented in this case, where a law enforcement officer looks only at images that have been previously hash-matched and not at other images or other communications.

In summary, Hartsock's email does not alter the Court's analysis of the *Franks* issue. After viewing the entire affidavit with the few inaccurate words discussed in Part I(C)(1) above removed, the Court concludes that its contents were accurate and did not in fact mislead the judge who issued the warrant. Further, there is no evidence that Hartsock *intended* to mislead the judge. Rather, the evidence in the affidavit was sufficient to establish probable cause to believe that someone at Rosenschein's Albuquerque address had possessed child pornography and at a minimum attempted to distribute it on Chatstep, and therefore there was probable cause for the warrant to issue.

5. Good Faith Doctrine

Alternatively, even if the search warrant affidavit had violated *Franks*, which the Court has concluded it did not, the search would still be valid under the good faith doctrine, which holds that even if a warrant is not supported by probable cause, evidence seized in good-faith reliance on that warrant is not subject to suppression. *United States v. Leon*, 468 U.S. 897, 922 (1984). The *Leon* Court held that the purpose of the exclusionary rule is to deter police misconduct, and that the suppression of evidence obtained pursuant to a warrant should be ordered only in the unusual cases in which exclusion will further the purposes of the exclusionary rule. *Id*. at 918. "Where an officer acting with objective good faith obtains a search warrant from a detached and neutral magistrate and the executing officers act within its scope, there is nothing to deter." *United States v. Nolan*, 199 F.3d 1180, 1184 (10th Cir. 1999); *United States v. Tuter*, 240 F.3d 1292, 1298-99 (10th Cir.2001). This is because "exclusion [is] our last resort, not our first impulse." *Herring v. United States*, 555 U.S. 135, 140 (2009) (quotations omitted).

However, an exception to this general rule is that "when the affidavit in support of the warrant is 'so lacking in indicia of probable cause as to render official belief in its existence unreasonable[,]'" the officer cannot be said to have acted in good-faith reliance on the magistrate's determination, and suppression is appropriate. *United States v. Danhauer*, 229 F.3d 1002, 1007 (10th Cir. 2000) (quoting *Leon*, 468 U.S. at 923). In other words, "[i]n the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *Leon*, 468 U.S. at 926. "[T]he analysis 'is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Massi*, 761 F.3d 512, 530 (5th Cir. 2014).

Rosenschein argues that the good faith exception does not apply because Hartsock knew or should have known that the grand jury subpoenas, which were based on ICAC's viewing of the hash-matched files, were illegal and that he only perpetuated that unconstitutional conduct by requesting a search warrant based on those illegal grand jury subpoenas. But as the Court already explained, the grand jury subpoenas were not improper due to Rosenschein's lack of cognizable privacy interest in photos uploaded to a chat room and the fact that ICAC repeated a prior private search by PhotoDNA. There is simply nothing in the record which suggests that Hartsock would have any reason to believe the subpoenas were illegally obtained. Further, no reasonable officer would have found clarity from the *Ackerman* opinion, which left open the question of whether a government entity violates the Fourth Amendment when it opens only the hash-matched image and does not view any other messages, emails, or attachments. *Ackerman*, 831 F.3d at 1306-07.

Thus, neither the *Ackerman* opinion nor Hartsock's email seeking guidance about the decision demonstrates bad faith.

Most telling on the issue of good faith is the fact that, in his affidavit seeking a search warrant, Hartsock recited the circumstances surrounding the state court subpoenas by which he came into possession of the CenturyLink information, as well as the fact that he opened and viewed the images before seeking the warrant. These facts demonstrate Hartsock's firmly held conviction that the subpoenas were valid and that his own viewing of the files was appropriate and lawful. Had he not held those beliefs, he would have had reason to either hide those facts or to expect that the judge issuing the search warrant would refuse to issue the search warrant.

The Court finds that Hartsock's reliance on the warrant was objectively reasonable. There was nothing in the warrant or otherwise known by him that would have made an objectively reasonable officer doubt the warrant's validity. Furthermore, there is no evidence in the record to indicate that any of the disqualifying scenarios, involving dishonest or misleading police conduct or the magistrate judge's abandonment of his or her role as independent arbiter are applicable to this case. Indeed, the hash match alone--without viewing the images--might establish sufficient probable cause to support the validity of the warrant. *See United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (stating that a hash value match from a reliable source could support the issuance of a warrant under the totality of the circumstances). Thus, the good faith exception applies.

II. Lack of Probable Cause and Sufficiency of the Warrant Affidavit

Rosenschein's *Motion to Suppress Evidence Due to Detective Hartsock's Unconstitutional Conduct* [Doc. 77], asserts the argument that Detective Kyle Hartsock improperly viewed images that Rosenschein uploaded to Chatstep without a warrant, and then sought a warrant to search Rosenschein's home based on viewing those images. Rosenschein contends that Hartsock's affidavit failed to inform the judge that he had viewed the images without a warrant, failed to give a detailed description of the images, and failed to attach the images to his affidavit. Rosenschein contends that without this information, there was no probable cause for the warrant. This motion was addressed by the Government in its combined response [Doc. 82] and by Rosenschein in his consolidated reply brief. [Doc. 86].

These arguments restate arguments already put forth by Rosenschein in his other motions to suppress, and the Court rejects them for the same reasons previously stated. Therefore, the motion to suppress will be denied.

IT IS THEREFORE ORDERED that:

(1) Rosenschein's *Motion to Suppress Evidence & Request for an Evidentiary Hearing under Franks v. Delaware* [Doc. 71] and Rosenschein's *Updated Motion to Suppress Illegally Obtained Evidence for Lack of Probable Cause* [Doc. 254] are **GRANTED IN PART** insofar as Rosenschein was granted the evidentiary hearing, but **DENIED IN PART** as to the suppression of evidence; and

(2) Defendant's *Motion to Suppress Evidence Due to Detective Hartsock's Unconstitutional Conduct* [Doc. 77] is **DENIED**.

SENIOR UNITED STATES DISTRICT JUDGE